Search Results

Results for "((('get request' counter<in>metadata) <and> (http<in>metadata))<and>..." e-mail

Your search matched **0** documents.

A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

((('get request' counter<in>metadata) <and> (http<in>metadata))<and> ('dos atta Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

☐ **Search Results**

Results for **"(('post request' <in>metadata) <and> (dos<in>metadata))"** e-mail
Your search matched **0** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» **Search Options**

View Session History

New Search

Modify Search

(('post request' <in>metadata) <and> (dos<in>metadata)) Search

☐ Check to search only within this results set

Display Format: ◉ Citation ○ Citation & Abstract

» **Key**

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistan search.

Search Results

Results for "(('denial-of-service' attack<in>metadata)) <and> (pyr >= 1950 <and> pyr &..." e-mail
Your search matched **24** of **1641691** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

(('denial-of-service' attack<in>metadata)) <and> (pyr >= 1950 <and> pyr <= 2000) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **Preventing denial-of-service attacks on a μ-kernel for WebOSes**
Liedtke, J.; Islam, N.; Jaeger, T.;
Operating Systems, 1997., The Sixth Workshop on Hot Topics in
5-6 May 1997 Page(s):73 - 79
Digital Object Identifier 10.1109/HOTOS.1997.595186
AbstractPlus | Full Text: PDF(528 KB) IEEE CNF
Rights and Permissions

2. **Distributed denial of service attacks**
Lau, F.; Rubin, S.H.; Smith, M.H.; Trajkovic, L.;
Systems, Man, and Cybernetics, 2000 IEEE International Conference on
Volume 3, 8-11 Oct. 2000 Page(s):2275 - 2280 vol.3
Digital Object Identifier 10.1109/ICSMC.2000.886455
AbstractPlus | Full Text: PDF(492 KB) IEEE CNF
Rights and Permissions

3. **Defeating distributed denial of service attacks**
Xianjun Geng; Whinston, A.B.;
IT Professional
Volume 2, Issue 4, July-Aug. 2000 Page(s):36 - 42
Digital Object Identifier 10.1109/6294.869381
AbstractPlus | Full Text: PDF(184 KB) IEEE JNL
Rights and Permissions

4. **Analysis of a denial of service attack on TCP**
Schuba, C.L.; Krsul, I.V.; Kuhn, M.G.; Spafford, E.H.; Sundaram, A.; Zamboni,
Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on
4-7 May 1997 Page(s):208 - 223
Digital Object Identifier 10.1109/SECPRI.1997.601338
AbstractPlus | Full Text: PDF(1112 KB) IEEE CNF
Rights and Permissions

5. **On the trail of intrusions into information systems**
Kent, S.;
Spectrum, IEEE
Volume 37, Issue 12, Dec. 2000 Page(s):52 - 56
Digital Object Identifier 10.1109/6.887597

AbstractPlus | Full Text: PDF(48 KB) IEEE JNL
Rights and Permissions

6. **Developing a distributed system for infrastructure protection**
Cybenko, G.; Guofei Jiang;
IT Professional
Volume 2, Issue 4, July-Aug. 2000 Page(s):17 - 23
Digital Object Identifier 10.1109/6294.869375
AbstractPlus | Full Text: PDF(180 KB) IEEE JNL
Rights and Permissions

7. **Secure quality of service handling: SQoSH**
Alexander, D.S.; Arbaugh, W.A.; Keromytis, A.D.; Muir, S.; Smith, J.M.;
Communications Magazine, IEEE
Volume 38, Issue 4, April 2000 Page(s):106 - 112
Digital Object Identifier 10.1109/35.833566
AbstractPlus | References | Full Text: PDF(64 KB) IEEE JNL
Rights and Permissions

8. **Spout: a transparent distributed execution engine for Java applets**
Tzi-Cker Chiueh; Sankaran, H.; Neogi, A.;
Distributed Computing Systems, 2000. Proceedings. 20th International Confer
10-13 April 2000 Page(s):394 - 401
Digital Object Identifier 10.1109/ICDCS.2000.840951
AbstractPlus | Full Text: PDF(88 KB) IEEE CNF
Rights and Permissions

9. **Analyzing single-server network inhibition**
Aura, T.; Bishop, M.; Sniegowski, D.;
Computer Security Foundations Workshop, 2000. CSFW-13. Proceedings. 13t
3-5 July 2000 Page(s):108 - 117
Digital Object Identifier 10.1109/CSFW.2000.856930
AbstractPlus | Full Text: PDF(276 KB) IEEE CNF
Rights and Permissions

10. **Malicious packet dropping: how it might impact the TCP performance an detect it**
Xiaobing Zhang; Wu, S.F.; Zhi Fu; Tsung-Li Wu;
Network Protocols, 2000. Proceedings. 2000 International Conference on
14-17 Nov. 2000 Page(s):263 - 272
Digital Object Identifier 10.1109/ICNP.2000.896310
AbstractPlus | Full Text: PDF(728 KB) IEEE CNF
Rights and Permissions

11. **Using conservation of flow as a security mechanism in network protocol**
Hughes, J.R.; Aura, T.; Bishop, M.;
Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium c
14-17 May 2000 Page(s):132 - 141
Digital Object Identifier 10.1109/SECPRI.2000.848451
AbstractPlus | Full Text: PDF(184 KB) IEEE CNF
Rights and Permissions

12. **A stateful inspection module architecture**
Noureldien, N.A.; Osman, I.M.;
TENCON 2000. Proceedings
Volume 2, 24-27 Sept. 2000 Page(s):259 - 265 vol.2
Digital Object Identifier 10.1109/TENCON.2000.888744
AbstractPlus | Full Text: PDF(484 KB) IEEE CNF
Rights and Permissions

13. **Resolution of ISAKMP/Oakley key-agreement protocol resistant against c attack**
Matsuura, K.; Imai, H.;
Internet Workshop, 1999. IWS 99
18-20 Feb. 1999 Page(s):17 - 24
Digital Object Identifier 10.1109/IWS.1999.810911
AbstractPlus | Full Text: PDF(576 KB) IEEE CNF
Rights and Permissions

14. **Vulnerabilities of reliable multicast protocols**
Parks, T.M.; Kassay, D.A.; Weinstein, C.J.;
Military Communications Conference, 1998. MILCOM 98. Proceedings., IEEE
Volume 3, 18-21 Oct. 1998 Page(s):934 - 938 vol.3
Digital Object Identifier 10.1109/MILCOM.1998.726977
AbstractPlus | Full Text: PDF(444 KB) IEEE CNF
Rights and Permissions

15. **A network version of the Pump**
Kang, M.H.; Moskowitz, I.S.; Lee, D.C.;
Security and Privacy, 1995. Proceedings., 1995 IEEE Symposium on
8-10 May 1995 Page(s):144 - 154
Digital Object Identifier 10.1109/SECPRI.1995.398929
AbstractPlus | Full Text: PDF(776 KB) IEEE CNF
Rights and Permissions

16. **A network pump**
Kang, M.H.; Moskowitz, I.S.; Lee, D.C.;
Software Engineering, IEEE Transactions on
Volume 22, Issue 5, May 1996 Page(s):329 - 338
Digital Object Identifier 10.1109/32.502225
AbstractPlus | References | Full Text: PDF(1000 KB) IEEE JNL
Rights and Permissions

17. **Distributed denial of service attacks and the zombie ant effect**
Elliott, J.;
IT Professional
Volume 2, Issue 2, March-April 2000 Page(s):55 - 57
Digital Object Identifier 10.1109/MITP.2000.839372
AbstractPlus | Full Text: PDF(332 KB) IEEE JNL
Rights and Permissions

18. **Denial-of-service attacks rip the internet**
Garber, L.;
Computer
Volume 33, Issue 4, April 2000 Page(s):12 - 17
Digital Object Identifier 10.1109/MC.2000.839316
AbstractPlus | Full Text: PDF(296 KB) IEEE JNL
Rights and Permissions

19. **Denial of service protection the nozzle**
Strother, E.;
Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference
11-15 Dec. 2000 Page(s):32 - 41
Digital Object Identifier 10.1109/ACSAC.2000.898855
AbstractPlus | Full Text: PDF(660 KB) IEEE CNF
Rights and Permissions

20. Securing ad hoc networks
Lidong Zhou; Haas, Z.J.;
Network, IEEE
Volume 13, Issue 6, Nov.-Dec. 1999 Page(s):24 - 30
Digital Object Identifier 10.1109/65.806983
AbstractPlus | Full Text: PDF(584 KB) IEEE JNL
Rights and Permissions

21. Techniques for intrusion-resistant ad hoc routing algorithms (TIARA)
Ramanujan, R.; Ahamad, A.; Bonney, J.; Hagelstrom, R.; Thurber, K.;
MILCOM 2000. 21st Century Military Communications Conference Proceedinc
Volume 2, 22-25 Oct. 2000 Page(s):660 - 664 vol.2
Digital Object Identifier 10.1109/MILCOM.2000.904011
AbstractPlus | Full Text: PDF(428 KB) IEEE CNF
Rights and Permissions

22. Statistical traffic modeling for network intrusion detection
Caberera, J.B.D.; Ravichandran, B.; Mehra, R.K.;
Modeling, Analysis and Simulation of Computer and Telecommunication Syste
Proceedings. 8th International Symposium on
29 Aug.-1 Sept. 2000 Page(s):466 - 473
Digital Object Identifier 10.1109/MASCOT.2000.876573
AbstractPlus | Full Text: PDF(644 KB) IEEE CNF
Rights and Permissions

23. Using Web technologies in two MLS environments: a security analysis
Niemeyer, R.E.;
Computer Security Applications Conference, 1997. Proceedings., 13th Annual
8-12 Dec. 1997 Page(s):205 - 214
Digital Object Identifier 10.1109/CSAC.1997.646191
AbstractPlus | Full Text: PDF(840 KB) IEEE CNF
Rights and Permissions

24. A case study of two NRL Pump prototypes
Kang, M.H.; Moskowitz, I.S.; Montrose, B.E.; Parsonese, J.J.;
Computer Security Applications Conference, 1996., 12th Annual
9-13 Dec. 1996 Page(s):32 - 43
Digital Object Identifier 10.1109/CSAC.1996.569667
AbstractPlus | Full Text: PDF(856 KB) IEEE CNF
Rights and Permissions

Published before December 2000
Terms used: **"denial of service attack strother nozzle**

Found **228** of **118,197**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown
Relevance scale

1 Inside Risks: denial-of-service attacks
Peter G. Neumann
April 2000 **Communications of the ACM**, Volume 43 Issue 4
Publisher: ACM Press
Full text available: pdf(49.45 KB) html(7.80 KB) Additional Information: full citation, citings, index terms

2 Internet security attacks at the basic levels
Marco de Vivo, Gabriela O. de Vivo, Germinal Isern
April 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 2
Publisher: ACM Press
Full text available: pdf(1.28 MB) Additional Information: full citation, abstract, references, citings

The Internet put the rest of the world at the reach of our computers. In the same way it also made our computers reachable by the rest of the world. Good news and bad news!. Over the last decade, the Internet has been subject to widespread security attacks. Besides the classical terms, new ones had to be found in order to designate a large collection of threats: *Worms, break-ins, hackers, crackers, hijacking, phrackers, spoofing, man-in-the-middle, password-sniffing, denial-of-service,* an ...

Keywords: Client-Server, Covert Channel, DNS, Denial of Service, Ethernet, Hijacking, ICMP, Kerberos, One-Time Password, Ping, RIP, Sniffing, Spoofing, TCP/IP

3 Denial of service
Roger M. Needham
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(277.12 KB) Additional Information: full citation, abstract, references, citings, index terms

The contractor uses the client, the network, and the server to give a service to the customer. We put it this way to emphasise that the denial of service against which we seek to protect is the denial of service to the customer, not to the client. The attack may

indeed consist of disabling or destroying the client, just as it may consist of interfering with the network or with the server. This paper does not consider issues of responsibility.

4 Practical network support for IP traceback

Stefan Savage, David Wetherall, Anna Karlin, Tom Anderson
August 2000 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication SIGCOMM '00**, Volume 30 Issue 4
Publisher: ACM Press

Full text available: pdf(167.15 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or ``spoofed'', source addresses. In this paper we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) trave ...

5 Denial of service: an example

Roger M. Needham
November 1994 **Communications of the ACM**, Volume 37 Issue 11
Publisher: ACM Press

Full text available: pdf(2.98 MB) Additional Information: full citation, references, citings, index terms

6 KHIP—a scalable protocol for secure multicast routing

Clay Shields, J. J. Garcia-Luna-Aceves
August 1999 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '99**, Volume 29 Issue 4
Publisher: ACM Press

Full text available: pdf(1.54 MB) Additional Information: full citation, abstract, references, citings, index terms

We present Keyed HIP (KHIP), a secure, hierarchical multicast routing protocol. We show that other shared-tree multicast routing protocols are subject to attacks against the multicast routing infrastructure that can isolate receivers or domains or introduce loops into the structure of the multicast routing tree. KHIP changes the multicast routing model so that only trusted members are able to join the multicast tree. This protects the multicast routing against attacks that could form branches to ...

7 Protecting routing infrastructures from denial of service using cooperative intrusion detection

Steven Cheung, Karl N. Levitt
January 1998 **Proceedings of the 1997 workshop on New security paradigms NSPW '97**
Publisher: ACM Press

Full text available: pdf(1.44 MB) Additional Information: full citation, references, citings, index terms

8 Report of the national workshop on internet voting: issues and research agenda

C. D. Mote
May 2000 **Proceedings of the 2000 annual national conference on Digital government research dg.o '00**

Publisher: Digital Government Research Center
Full text available: pdf(539.99 KB) Additional Information: full citation, abstract

As use of the Internet in commerce, education and personal communication has become common, the question of Internet voting in local and national elections naturally arises. In addition to adding convenience and precision, some believe that Internet voting may reverse the historical and downward trend of voter turnout in the United States. For these reasons President Clinton issued a memorandum in December 1999 requesting that the National Science Foundation examine the feasibility of online (In ...

9 Undetectable on-line password guessing attacks
Yun Ding, Patrick Horster
October 1995 **ACM SIGOPS Operating Systems Review**, Volume 29 Issue 4
Publisher: ACM Press
Full text available: pdf(621.20 KB) Additional Information: full citation, abstract, citings, index terms

Several 3-party-based authentication protocols have been proposed, which are resistant to off-line password guessing attacks. We show that they are not resistant to a new type of attack called "undetectable on-line password guessing attack". The authentication server is not able to notice this kind of attack from the clients' (attacker's) requests, because they don't include enough information about the clients (or attacker). Either freshness or authenticity of these requests is not guaranteed. ...

10 Security problems in the TCP/IP protocol suite
S. M. Bellovin
April 1989 **ACM SIGCOMM Computer Communication Review**, Volume 19 Issue 2
Publisher: ACM Press
Full text available: pdf(2.72 MB) Additional Information: full citation, abstract, citings, index terms

The TCP/IP protocol suite, which is very widely used today, was developed under the sponsorship of the Department of Defense. Despite that, there are a number of serious security flaws inherent in the protocols, regardless of the correctness of any implementations. We describe a variety of attacks based on these flaws, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks. We also present defenses against these attacks, and conclude with a discu ...

11 Testing and evaluating computer intrusion detection systems
Robert Durst, Terrence Champion, Brian Witten, Eric Miller, Luigi Spagnuolo
July 1999 **Communications of the ACM**, Volume 42 Issue 7
Publisher: ACM Press
Full text available: pdf(220.41 KB) html(35.64 KB) Additional Information: full citation, citings, index terms, review

12 Inside risks: semantic network attacks
Bruce Schneier
December 2000 **Communications of the ACM**, Volume 43 Issue 12
Publisher: ACM Press
Full text available: pdf(52.74 KB) html(8.05 KB) Additional Information: full citation, citings, index terms

13 Security Mechanisms in High-Level Network Protocols
Victor L. Voydock, Stephen T. Kent

June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

14 A high-performance network intrusion detection system
R. Sekar, Y. Guang, S. Verma, T. Shanbhag
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we present a new approach for network intrusion detection based on concise specifications that characterize normal and abnormal network packet sequences. Our specification language is geared for a robust network intrusion detection by enforcing a strict type discipline via a combination of static and dynamic type checking. Unlike most previous approaches in network intrusion detection, our approach can easily support new network protocols as information relating to the protoco ...

15 Using router stamping to identify the source of IP packets
Thomas W. Doeppner, Philip N. Klein, Andrew Koyfman
November 2000 **Proceedings of the 7th ACM conference on Computer and communications security CCS '00**
Publisher: ACM Press
Full text available: pdf(283.11 KB) Additional Information: full citation, references, citings, index terms

16 Papers: Internet vulnerabilities related to TCP/IP and T/TCP
Marco de Vivo, Gabriela O. de Vivo, Roberto Koeneke, Germinal Isern
January 1999 **ACM SIGCOMM Computer Communication Review**, Volume 29 Issue 1
Publisher: ACM Press
Full text available: pdf(561.55 KB) Additional Information: full citation, abstract, references

The Internet put the rest of the world at the reach of our computers. In the same way it also made our computers reachable by the rest of the world. Good news and bad news! Over the last decade, the Internet has been subject to widespread security attacks. Besides the classical terms, new ones had to be found in order to designate a large collection of threats: *Worms, break-ins, hackers, crackers, hijacking, phrackers, spoofing, man-in-the-middle, password-sniffing, denial-of-service*, and ...

Keywords: Denial of Service, SYN Attack, Sniffing, Spoofing, T/TCP, TCP/IP

17 Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory
November 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 4
Publisher: ACM Press
Full text available: pdf(156.16 KB) Additional Information: full citation, abstract, references, citings, index terms, review

In 1998 and again in 1999, the Lincoln Laboratory of MIT conducted a comparative evaluation of intrusion detection systems (IDSs) developed under DARPA funding. While this evaluation represents a significant and monumental undertaking, there are a number

of issues associated with its design and execution that remain unsettled. Some methodologies used in the evaluation are questionable and may have biased its results. One problem is that the evaluators have published relatively little concer ...

Keywords: computer security, intrusion detection, receiver operating curves (ROC), software evaluation

18 An end-to-end approach to host mobility

Alex C. Snoeren, Hari Balakrishnan
August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking MobiCom '00**
Publisher: ACM Press

Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references, citings, index terms

We present the design and implementation of an end-to-end architecture for Internet host mobility using dynamic updates to the Domain Name System (DNS) to track host location. Existing TCP connections are retained using secure and efficient connection migration, enabling established connections to seamlessly negotiate a change in endpoint IP addresses without the need for a third party. Our architecture is secure—name updates are effected via the secure DNS update protocol, while TCP ...

19 Intrusion detection in wireless ad-hoc networks

Yongguang Zhang, Wenke Lee
August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking MobiCom '00**
Publisher: ACM Press

Full text available: pdf(936.44 KB) Additional Information: full citation, abstract, references, citings, index terms

As the recent denial-of-service attacks on several major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the intrusion detection techniques developed on a fixed wired network are not applicable in this new environment. Ho ...

20 On the functional relation between security and dependability impairments

Erland Jonsson, Lars Strömberg, Stefan Lindskog
September 1999 **Proceedings of the 1999 workshop on New security paradigms NSPW '99**
Publisher: ACM Press

Full text available: pdf(769.34 KB) Additional Information: full citation, references, citings, index terms

Keywords: dependability, impairment, intrusion, modeling, security, terminology, threat, vulnerability